Robin L. Cohen (rcohen@kasowitz.com)
Adam S. Ziffer (aziffer@kasowitz.com)
Alexander M. Sugzda (asugzda@kasowitz.com)
KASOWITZ, BENSON, TORRES &
FRIEDMAN LLP
1633 Broadway
New York, New York 10019
Tel: (212) 506-1700
Fax: (212) 506-1800
Attorneys for Plaintiff Medidata Solutions, Inc.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MEDIDATA SOLUTIONS, INC. Plaintiff, v. FEDERAL INSURANCE COMPANY, Defendant.	Civil Action No.: 1:15-cv-00907-ALC

PLAINTIFF MEDIDATA SOLUTIONS, INC.'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

Plaintiff Medidata Solutions, Inc. ("Medidata"), submits this memorandum of law in support of its motion pursuant to Federal Rule of Civil Procedure 56 for summary judgment against Defendant Federal Insurance Company ("Federal").

PRELIMINARY STATEMENT

Medidata provides cloud-based applications and analytics to allow medical scientists engaged in clinical trials to more quickly, powerfully, and efficiently collect and process the data generated during trials. In the summer of 2014, it was the victim of a $5 million computer fraud. An unknown perpetrator fraudulently manipulated the sender's email address in a series of emails, which tricked Medidata's Google-based email system into creating the impression that the emails came from Medidata's [redacted]. When the imposter's fraudulently manipulated emails entered Medidata's computer system, they caused the system to display the [redacted] picture, full name, and actual email address in the emails' "From" line. The imposter also electronically signed the emails as if he or she was Medidata's [redacted]. Effectively disguised by this manipulation of Medidata's computer system and use of the [redacted] electronic signature, the imposter was able to direct certain Medidata employees to authorize a nearly $5 million wire transfer, ostensibly to support an overseas acquisition. Although the company and the FBI investigated the fraud, the funds were never recovered and the perpetrators were never caught.

Fortunately, like any prudent company, Medidata had purchased insurance coverage to protect it from just such losses. Under a 2014 Crime Coverage insurance policy sold by defendant Federal, Medidata is insured for a number of types of loss, several of which are directly applicable to Medidata's loss resulting from the fraud. Specifically, the policy covers losses resulting from Computer Fraud, Funds Transfer Fraud, and Forgery.

Unfortunately, even though Federal concedes that most of the policy requirements for payment of Medidata's claim with respect to the fraud have been met, Federal nonetheless has refused to pay that claim, ignoring the policy's plain language and imposing additional restrictions on each grant of coverage. An application of the policy's actual terms to the undisputed facts of the fraud that resulted in Medidata's loss, however, entitles Medidata to judgment as a matter of law under each of the three coverage provisions identified above.

First, the policy's Computer Fraud Coverage covers losses arising from the fraudulent entry of data or change of data in Medidata's computer systems, both of which occurred as part of the fraud. Federal argues that the Computer Fraud Coverage is limited to instances in which the Medidata computer system itself is "hacked" – a term and a concept that does not appear in the policy. Indeed, the cases that Federal has offered to supposedly support its hacker requirement expressly recognize that Computer Fraud Coverage is fully applicable to the "imposter" fraud suffered by Medidata. Federal's alternate attempt to avoid coverage under this provision – its argument that Medidata's loss did not result directly from the manipulation of the sender's email address – is contrary to the undisputed fact that all three Medidata employees who were convinced to authorize the wire transfer did so precisely because the fraudulent emails directing them to do so displayed the [redacted] name, email address, and picture in the same manner as his legitimate emails.

Second, the policy's Funds Transfer Fraud Coverage provides coverage for losses arising from electronic fund transfers made without Medidata's knowledge or consent – again, precisely the event at the heart of the fraud. Federal argues that despite the fact that the fraudulent instructions were initially given to Medidata employees by an imposter, because the ultimate transfer instructions given to Medidata's bank were authorized by those employees, they were

given with the knowledge and consent of Medidata itself. In fact, however, the three employees were co-opted by the imposter, were only "purportedly" acting on behalf of Medidata, and were merely the conduits for the fraudulent instructions. Having been duped and their actions following the instructions of the imposter, there can be no argument that the employees' instructions were issued with Medidata's "knowledge and consent." Moreover, unlike the insurers in the cases it cites, Federal did not include limiting language in its policy requiring that the transmittal itself be fraudulent or excluding transfers initiated by authorized representatives. As a matter of law, it cannot add those restrictions to the policy by implication now.

Finally, the policy's Forgery Coverage applies because Medidata's loss also resulted from the imposter's use of an electronic signature of Medidata's [redacted] with the intent to deceive. Federal's position that there is no coverage under this provision because the forgery at issue was not of a financial instrument fails for two reasons. First, financial instrument is defined in the policy as an "order or direction to pay a sum certain." One of the emails that the imposter electronically signed with the name of Medidata's [redacted] directed the recipients to pay $4,770,226 to the perpetrators' overseas account, and thus meets that definition. Second, the policy does not clearly require that the forgery be of a financial instrument but instead provides coverage for either a forgery (as defined therein) *or* alteration of a financial instrument. Because the policy can reasonably be read as providing two paths to coverage for Forgery, and Medidata's claim satisfies both, this coverage applies as well.

STATEMENT OF FACTS

Medidata was founded in 1999 to provide solutions for the inefficiencies and delays that routinely faced scientists in clinical trials. Medidata now employs over 1,000 people working to provide cloud-based applications and analytics to allow clinical trial teams to more quickly, powerfully, and efficiently collect and process the data generated during trials. With assistance

from Medidata, researchers are able to pursue breakthroughs in the life sciences at a lower cost, lower risk, and with greater speed than ever before.

A. The Federal Insurance Policy

In exchange for a $31,400 premium, Medidata purchased Federal Executive Protection Portfolio Policy No. 8212-1392 (the "Policy") from Federal covering the policy period June 25, 2014 to June 25, 2015. (Joint Exhibit Stipulation ("Ex. Stip.") Ex. 1, at FIC001322, 1327.) The Policy contains a Crime Coverage Section that contains ten Insuring Clauses providing coverage for loss caused by various criminal acts, including Forgery Coverage Insuring Clause 4, Computer Fraud Coverage Insuring Clause 5, and Funds Transfer Fraud Coverage Insuring Clause 6. (*Id.* at FIC001340.) The Policy provides one "Limit of Liability" applicable to its Forgery Coverage, Computer Fraud Coverage, and Funds Transfer Fraud Coverage of $5,000,000, subject to a $50,000 retention. (*Id.*)

The Policy contains various definitions applicable to all of its Crime Coverage parts which are relevant to the issues raised in this motion. The Policy defines "**Organization**" as "any organization designated in Item 4 of the Declarations for this coverage section."[1] (*Id.* at FIC001346.) Item 4, in turn, lists "Medidate [sic] Solutions, Inc., and its subsidiaries" as a covered Organization. (*Id.* at FIC001340.) The Policy defines "**Third Party**" as "a natural person other than: (a) an **Employee**; or (b) a natural person acting in collusion with an **Employee**." (*Id.* at FIC001347.) The definition of "**Computer System**" includes "a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are: (a) owned

[1] All emphasized terms appear in boldface in the Policy.

and operated by an **Organization**; (b) leased and operated by an **Organization**; or (c) utilized by an **Organization**." (*Id.* at FIC001374.)

1. Computer Fraud Coverage

The Policy's Computer Fraud Coverage, Insuring Clause 5, covers "direct loss of **Money**, **Securities** or **Property** sustained by an **Organization** resulting from **Computer Fraud** committed by a **Third Party**." (*Id.* at FIC001342.) The Policy defines "**Computer Fraud**" as: "[T]he unlawful taking or the fraudulently induced transfer of **Money**, **Securities** or **Property** resulting from a **Computer Violation**." (*Id.* at FIC001343.) A "**Computer Violation**" includes both "the fraudulent: (a) entry of **Data** into . . . a **Computer System**; [and] (b) change to **Data** elements or program logic of a **Computer System**, which is kept in machine readable format . . . directed against an **Organization**." (*Id.* at FIC001343-44.) The Policy defines "**Data**" broadly to include any "representation of information." (*Id.* at FIC001344.)

2. Funds Transfer Fraud Coverage

The Policy's Funds Transfer Fraud Coverage, Insuring Clause 6, covers "direct loss of **Money** or **Securities** sustained by an **Organization** resulting from **Funds Transfer Fraud** committed by a **Third Party**." (*Id.* at FIC001342.) The Policy defines "**Funds Transfer Fraud**" as: "[F]raudulent electronic . . . instructions . . . purportedly issued by an **Organization**, and issued to a financial institution directing such institution to transfer, pay or deliver **Money** or **Securities** from any account maintained by such **Organization** at such institution, without such **Organization's** knowledge or consent." (*Id.* at FIC001345.)

3. Forgery Coverage

The Policy's Forgery Coverage, Insuring Clause 4, covers "direct loss sustained by an **Organization** resulting from **Forgery** or alteration of a **Financial Instrument** committed by a **Third Party**" and provides a non-exclusive list of examples. (*Id.* at FIC001342.) "**Forgery**" is

defined as "the signing of the name of another natural person . . . with the intent to deceive . . . . Mechanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures." (*Id.* at FIC001345.)

B. Medidata's Email System

Medidata uses Google's Gmail platform for its corporate email. (Affidavit of Glenn Watt, dated Aug. 11, 2015 ("Watt Aff.") ¶ 2.) Medidata employees' email addresses generally consist of their first initial and last name, followed by the domain name "mdsol.com" (not "gmail.com"). (*Id.* ¶ 3.) When a person emails a Medidata employee at their Medidata email address, the message goes to Google computer servers, where it is processed and then stored on those servers. (*Id.* ¶ 4.) After an incoming email is processed, Google's servers then enable it to be displayed in the Medidata employee's email account, which can then be accessed by Medidata employees on computers owned by Medidata at Medidata's offices. (*Id.* ¶ 7.) When the information in an incoming email is processed by Google's servers, the Gmail system displays the sender's email address in the "From" line of the email. (*Id.* ¶ 8.)

One feature of Gmail is that Google's email system will compare an incoming email's sender's email address to all Medidata employee profiles contained in its system for a match. (*Id.* ¶ 9.) If Google's Gmail system matches the email address of a sender with a Medidata employee account, it will display the sender's full name in the "From" line, followed by the sender's "@mdsol.com" email in angled brackets. (*Id.* ¶¶ 8, 10.) Furthermore, if a picture has been associated with that Medidata employee's account, the email system will automatically display that picture next to the sender's name and email address in the "From" line. (*Id.* ¶ 10.)

C. The Fraud Perpetrated against Medidata

In the summer of 2014, company leadership briefed employees in Medidata's finance department on short-term plans for the future of the company, and emphasized possible

acquisitions. (Ex. Stip. Ex. 19, Deposition of [redacted] 36:25-37:17, June 24, 2015 ("[redacted] Dep."); Ex. Stip. Ex. 21, Deposition of [redacted] 21:2-8, 34:22-35:12, June 25, 2015 ("[redacted] Dep."); Ex. Stip. Ex. 20, Deposition of [redacted] 22:24-24:2, 25:2-19, June 25, 2015 ("[redacted] Dep.").) In connection with that briefing, personnel in the company's finance and accounting departments were told to be prepared to assist with significant transactions on an urgent basis. ([redacted] Dep. 36:25-37:17; [redacted] Dep. 21:2-8, 34:22-35:12; [redacted] Dep. 22:24-24:2, 25:2-19.)

At 11:12 AM September 16, 2014, Medidata [redacted] employee [redacted] ("[redacted]") received an email from an imposter (the "Imposter") purporting to be Medidata [redacted]. (Ex. Stip. Ex. 2, at MED_0000816 (the "11:12 Email")); *see also* Watt Aff. ¶ 12, Ex. Stip. Ex. 23, Deposition of Michael Maillet 153:4-10, July 9, 2015 ("Maillet Dep.").) The Imposter fraudulently manipulated the sender's address of the 11:12 Email to appear as if it was sent by [redacted] real email address at Medidata. When Google's server processed the manipulated email that had been entered into its system, it recognized the sender's email address, and displayed the following in the email's "From" line: "[redacted]." (Ex. Stip. Ex. 2, at MED_0000816.)[2] It also automatically added [redacted] picture next to the "From" line, further making the email appear authentic. (*Id.*)

The 11:12 Email stated that Medidata was on the verge of an acquisition and that [redacted] would need to work with an attorney named Michael Meyer (the "Fake Attorney") to provide information to finalize the deal. (*Id.*) The Imposter cautioned that the deal was "extremely confidential" and instructed [redacted] "to keep complete silence and work exclusively with

[2] Federal does not contest that the Medidata recipients saw the color versions of the emails.

Michael." (*Id.*) The Imposter electronically signed the email "[redacted]." (*Id.* Ex. 3, at MED_0002113.)

[redacted] responded within minutes to the 11:12 Email and stated she would "assist in any way [she] can." (*Id.* Ex. 4, at MED_0002112.) [redacted] communicated with the Fake Attorney and informed him that a wire could be processed in JPMorgan Chase's online system any time before 10 PM, but that two authorized signatories would be required to approve the wire after it was prepared. (*Id.* Ex. 5, at MED_0002096.) [redacted] identified three authorized signatories, including [redacted], and Stephen Davis, Treasurer. (*Id.*; [redacted] Dep. 11:3-5; [redacted] Dep. 9:22-24.) [redacted] explained to the Fake Attorney that she needed the instruction for the transfer to come from [redacted] himself. ([redacted] Dep. 34:14-21.)

The Imposter then sent an email directly to [redacted] and [redacted]. (Ex. Stip. Ex. 6, at MED_0001025.) Again, although [redacted] did not send this email, because the Imposter fraudulently manipulated the sender's email address, Google's email system added [redacted] full name and picture adjacent to the "From" line. (*Id.*) In the email, the Imposter told [redacted], and [redacted] that he "need[ed] you to process and approve a payment on my behalf." (*Id.*) He asked [redacted] and [redacted] to keep the matter confidential until a public announcement was made. (*Id.*) The Imposter electronically signed the email "[redacted]." (*Id.* Ex. 7, at MED_0002095.)

At 3:52 PM the Imposter emailed [redacted] the "beneficiary details" she would need to prepare the wire, including the name of the bank in China, account number, and routing information for the transfer, and instructed [redacted] to wire the amount of $4,770,226.00. (*Id.* Ex. 8, at MED_0001045.) Once again, due to the Imposter's fraudulent manipulation of the sender's

email address, Google's email system displayed "[redacted]" in the "From" line and displayed his picture. (Watt Aff. ¶¶ 8-10; Ex. Stip. Ex. 8, at MED_0001045.) [redacted] used those instructions to prepare the wire in the JPMorgan Chase online system. ([redacted] Dep. 47:2-8.) [redacted] approved and [redacted] released the wire in the JPMorgan Chase online system, and the $4,770,226.00 was wired in accordance with the Imposter's fraudulent instructions. (Ex. Stip. Ex. 10, at MED_0000021.) All three employees confirmed to their satisfaction that the instruction came from [redacted] before they proceeded with their roles with respect to the transfer. ([redacted] Dep. 64:12-65:2; [redacted] Dep. 67:9-68:3; [redacted] Dep. 29:17-25.) Medidata did not purchase or receive anything in exchange for the funds transferred. (Maillet Dep. 179:19-180:2.)

Ultimately, Medidata employees discovered that this wire was not authorized and that the company had been defrauded. ([redacted] Dep. 63:9-64:18.) Medidata reported the fraud to the FBI, but the investigation that followed did not result in identifying any of the perpetrators of the fraud or recovery of the transferred funds. Medidata also hired outside counsel to investigate the circumstances surrounding the fraud. Neither outside counsel's investigation nor the investigation Federal conducted after receiving the claim for coverage revealed any fraudulent, dishonest, or criminal act by an authorized representative of Medidata. (Maillet Dep. 125:12-20.)

D. Medidata's Claim for Coverage

On September 25, 2014, Medidata notified Federal of the loss, and made a claim under the Policy for the lost funds. (Ex. Stip. Ex. 11, at FIC000733.) Federal assigned regional claims technician Michael Maillet ("Maillet"), who has the most experience of any Chubb claims examiner with respect to email fraud claims, to investigate. (Maillet Dep. 105:25-106:6.) Maillet's subsequent investigation confirmed that Medidata employees "acted upon a series of

fraudulent emails purporting to be from the [redacted] of Medidata, [redacted] . . . ." (Ex. Stip. Ex. 12, at FIC000045; Maillet Dep. 42:15-43:11.) Medidata cooperated with Federal's investigation, including its voluminous requests for documents and information. (Ex. Stip. Ex. 13, at FIC000714; Maillet Dep. 136:20-137:2.)

On December 24, 2014, Federal notified Medidata that it was denying Medidata's claim for coverage under the Policy. (Ex. Stip. Ex. 12, at FIC000045.) Federal rejected Medidata's claim under the Computer Fraud Coverage based on the assertion that (1) there had been no "fraudulent entry of **Data**" because the email inboxes of the Medidata employees were open to the public; and (2) there had been no "change to **Data** elements" because Federal found no evidence that the perpetrators of the fraud changed any preexisting data in committing the fraud. (*Id.* at FIC000048-49.) Federal further rejected Medidata's claim under the Funds Transfer Fraud Coverage on the supposed ground that the wire transfer had been authorized by Medidata employees and thus was made with the knowledge and consent of Medidata. (*Id.* at FIC000049.) Finally, Federal rejected Medidata's claim for Forgery Coverage because it argued that the emails were not signed, and even if they were, the emails did not meet the Policy's definition of a Financial Instrument. (*Id.* at FIC000048.) In addition, Federal based its denial of both the Forgery Coverage and the Computer Fraud Coverage claims on the assertion that the emails did not directly cause Medidata's loss, because no loss would have taken place if Medidata employees had not acted on the instructions contained in those emails. (*Id.* at FIC000048-49.)

On January 13, 2015, Medidata sent a letter responding to the denial and setting forth the basis for coverage under the Policy. (*Id.* Ex. 14.) Federal replied on January 30, 2015**,** reasserting its denial of coverage for the claim. (*Id.* Ex. 15.)

ARGUMENT

I. SUMMARY JUDGMENT STANDARD

Under Rule 56(a) of the Federal Rules of Civil Procedure, a court may grant summary judgment if the record "shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). Summary judgment is an expeditious and efficient way to resolve as a matter of law disputes that do not involve genuine issues of material fact and are fit for judicial resolution without the need for a trial. *See Celotex Corp. v. Catrett*, 477 U.S. 317, 327 (1986) (explaining summary judgment is an "integral part of the Federal Rules as a whole, which are designed to secure the just, speedy and inexpensive determination of every action" (internal quotation marks omitted)). While protecting the rights of the non-moving party, summary judgment gives the court an opportunity, at an early point in the litigation, to dispose of factually unsupported defenses, avoiding "further litigation on an issue with an unalterably predetermined outcome." *AIU N. Am., Inc. v. Caisse Franco Neerlandaise de Cautionnements*, 72 F. Supp. 2d 350, 352-53 (S.D.N.Y. 1999); *see also Celotex*, 477 U.S. at 323-24.

The moving party has the burden of demonstrating "the absence of a genuine issue of material fact." *Celotex*, 477 U.S. at 323. To avoid summary judgment, a party must "do more than simply show that there is some metaphysical doubt as to the material facts." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986). Instead, the party "must set forth specific facts showing that there is a genuine issue for trial," through affidavits or other evidence, as opposed to allegations or denials in the pleadings. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 250 (1986) (internal quotation marks omitted). Speculation, conclusory allegations, and conjecture are not enough to raise genuine issues of fact. *Knight v. U.S. Fire Ins. Co.*, 804 F.2d 9, 12 (2d Cir. 1986) (citing *Quarles v. Gen. Motors Corp.*, 758 F.2d 839, 840

(2d Cir. 1985) (per curiam)). "'[T]he mere existence of some alleged factual dispute between the parties' alone will not defeat a properly supported motion for summary judgment, and '[i]f the evidence is merely colorable, or is not significantly probative, summary judgment may be granted.'" *Meyer v. U.S. Tennis Ass'n*, No. 1:11-cv-06268(ALC)(MHD), 2014 WL 4495185, at *5 (S.D.N.Y. Sept. 11, 2014) (quoting *Anderson*, 477 U.S. at 249-50). New York courts have long observed that summary judgment is particularly well-suited to resolve issues of insurance policy construction. *See, e.g.*, *Mazzuoccolo v. Cinelli*, 245 A.D.2d 245, 246-47 (1st Dep't 1997) ("Unambiguous provisions of an insurance contract, as with any written contract, must be given their plain and ordinary meaning and the interpretation of such provisions is a question of law for the court." (citation omitted)).

Federal's Policy is a standard form policy sold to many other policyholders. (Ex. Stip. Ex. 22, Deposition of Christopher Arehart 40:20-41:4, July 9, 2015 ("Arehart Dep.").) The terms and conditions of the Policy, including the endorsements, were entirely drafted or selected by Federal and were not the product of any negotiation between Medidata and Federal. (*Id.* 40:7-12, 43:10-44:2.) Therefore, should the Court find any language in the Policy to be ambiguous, which includes any language for which the court finds Medidata and Federal have both proffered reasonable but conflicting interpretations, the language must be interpreted in Medidata's favor and against the sole drafter, Federal. *See Morgan Stanley Grp. Inc. v. New England Ins. Co.*, 225 F.3d 270, 275-76 (2d Cir. 2000) (explaining that if an insurance policy term is ambiguous and extrinsic evidence does not resolve the ambiguity, the court can apply the rule of contra preferentem, "which generally provides that where an insurer drafts a policy any ambiguity in the policy should be resolved in favor of the insured" (internal quotation marks omitted)).

II. THE POLICY'S COMPUTER FRAUD COVERAGE APPLIES TO MEDIDATA'S LOSS

Federal has not disputed, and cannot dispute, that virtually all of the Policy requirements for Computer Fraud Coverage are met. In particular Federal does not dispute that Medidata is an Organization under the Policy, that it suffered a loss of Money, or that that loss resulted from a fraud committed by a Third Party.

Moreover, contrary to Federal's position, as a matter of law and undisputed fact, Medidata suffered a "direct loss . . . resulting" from the fraudulent emails. (Ex. Stip. Ex. 1, at FIC001342.) But for the emails from the Imposter, the loss would not have occurred. [redacted], and [redacted] all testified that they would not have prepared, approved, or released the wire if they were not convinced that the instruction to do so came from [redacted], and that the fraudulent emails provided the linchpin for their belief. ([redacted] Dep. 64:12-65:2; [redacted] Dep. 67:9-68:3; [redacted] Dep. 29:17-25.) Even Federal's claims handler acknowledged that the emails from the Imposter were the first cause in a chain of causal events that led to the transfer and Medidata's loss (Maillet Dep. 103:24-104:18), and that Medidata employees "acted upon a series of fraudulent emails purporting to be from the [redacted] of Medidata, [redacted] . . . ." (Ex. Stip. Ex. 12, at FIC000045; Maillet Dep. 42:15-43:11).

This satisfies the standard established in the Second Circuit for "direct loss" language in an insurance policy. *See FDIC v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 205 F.3d 66, 76 (2d Cir. 2000) (finding a bank's loss was directly caused by nondisclosure of trustee when record showed bank would not have made the loan in question had trustee disclosed the information known about the loan recipient). In *FDIC*, a bank employee charged with approving loans failed to disclose to the bank his knowledge that the construction manager for a real-estate-venture-borrower had engaged in improper and illegal activities. *Id.* 68-69. The court evaluated whether

the employee's fraudulent nondisclosure caused the loss, as opposed to the construction manager's improper and illegal activities, or even the failure of the real-estate venture to repay the loan. *Id.* at 76. The court held that direct cause could be satisfied if the bank could demonstrate that it would not have made the loan in the absence of the fraud. *Id.* As applied here, the Court should hold as a matter of law that in the absence of the fraudulent emails, Medidata would not have transferred the $4.8 million, and would not have suffered its loss.

Thus, as a matter of law, Medidata's loss was directly caused by the fraud. Furthermore, Medidata's loss was directly caused by a Computer Fraud as defined in the Policy, and more specifically, Medidata suffered a fraudulently induced transfer of Money resulting from a Computer Violation. Both of the first two categories of Computer Violation are satisfied as a matter of law: "[T]he fraudulent (a) entry of **Data** into . . . a **Computer System**; [and] (b) change to **Data** elements . . . of a **Computer System** . . . directed against an **Organization**."[3] (Ex. Stip. Ex. 1, at FIC001343-44.)

A. Medidata's Loss Was Directly Caused by Fraudulent Entry of Data into a Computer System

Federal has not disputed that the sender's email address, the email address and name that appears in the "From" line of an email, and an individual's picture, are all representations of information, qualifying as Data under the Policy. (*See* Maillet Dep. 57:11-17.) In a genuine email, the email address of the sender appears in the "From" line of the email. (Maillet Dep. 34:7-15.) In the "spoofed" emails from the Imposter, the perpetrators of the Fraud substituted fraudulent data – the email address "[redacted]" – for the actual email address of the true sender. (Ex. Stip. Ex. 2, at MED_0000816; *id.* Ex. 6, at MED_0001025; *id.* Ex. 8, at

[3] The Policy defines "**Data**" broadly to include any "representation of information." (Ex. Stip. Ex. 1, at FIC001344.)

MED_0001045; Maillet Dep. 78:4-15.) When the three fraudulent emails were processed by Google's email system, the Computer System displayed [redacted] full name and picture even though [redacted] did not send the emails. (Watt Aff. ¶ 12.) When the Imposter sent the spoofed emails to [redacted] and [redacted] Data (the sender's email address) was fraudulently entered into a covered Computer System.[4] The Computer System recognized the (fraudulent) email address, and consequently displayed [redacted] name in the "From" section of the employees' Gmail inboxes and added the picture of [redacted] next to the "From" line of each of the fraudulent emails. The plain language of the Policy's definition of Computer Fraud requiring fraudulent entry of Data into a Computer System, that directly caused Medidata's loss, applies as a matter of law.

In its letter reaffirming its denial of Medidata's claim, Federal relied primarily on two inapt cases for the proposition that the Imposter's email did not constitute the fraudulent entry of Data. (Ex. Stip. Ex. 15, at FIC000005.) Neither case involved perpetrators who were strangers to the victim or the unauthorized manipulation of the computer system to achieve the fraud; to the contrary, they both involved fraudulent data entered into a computer system by an *authorized* user of the system. In *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, PA*, 38 Misc. 3d 859 (N.Y. Sup. Ct., N.Y. Cnty. 2013), *aff'd*, 110 A.D.3d 434 (1st Dep't 2013), *aff'd*, No. APL-2014-00133, __ N.E.3d ___, 2015 WL 3885816 (N.Y. June 25, 2015) ("*Universal*"), the policyholder sought reimbursement from the government on behalf of healthcare providers who were authorized to submit claims via access to Universal's computer

[4] Federal has not disputed that the Policy's definition of Computer System is satisfied by Medidata's use of Gmail. It cannot, as the Google servers that process and store Medidata's email constitute input, output, processing, storage, off-line media library and communication facilities that are utilized by Medidata, and are connected to computers that are owned and operated by Medidata. (Watt Aff. ¶ 5.) The emails are then viewed on the computers of Medidata employees, at Medidata's offices, which computers are owned by Medidata. (Watt Aff. ¶ 7; Maillet Dep. 153:15-20.)

system; at some point certain of those authorized users submitted false claims for fictitious services that they never performed. 38 Misc. 3d at 860-61. Similarly, in *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, No. CV 13-5039-JFW (MRWx), 2014 WL 3844627, at *1-2 (C.D. Cal. July 17, 2014) ("*Pestmaster*"), a payroll administrator who was authorized to directly withdraw funds from the policyholder's bank account to meet payroll obligations instead made off with the funds he withdrew.

Both *Universal* and *Pestmaster* concern *legitimate* entry into a Computer System of the policyholder, and a subsequent misuse of that legitimate entry. In contrast, here, the *entry* into the Computer System by the Imposter was itself unauthorized and fraudulent, and the Imposter manipulated Medidata's computer system to achieve the fraud. The trial court in *Universal* expressly distinguished between the "authorized user" access where the computer system "was otherwise properly utilized," and "misuse or manipulation of the system itself" by an "unauthorized user" or "unauthorized data." 38 Misc. 3d at 863.

In support of that distinction, the *Universal* court cited as "instructive" the ruling in *Morgan Stanley Dean Witter v. Chubb Group of Insurance Companies*, No. UNN-L-2928-01, 2004 WL 5352285 (N.J. Super. Ct. Law Div. Feb. 17, 2004), *aff'd in relevant part*, 2005 WL 3242234 (N.J. Super. Ct. App. Div. Dec. 2, 2005). The *Morgan Stanley* court described the "overall thrust" of a policy's coverage for "fraudulent input of electronic data into a customer communication system" as insuring "against computer hackers *or imposters*."[5] *Morgan Stanley*, 2004 WL 5352285, at *9 (emphasis added). The *Morgan Stanley* court went on to conclude that "[s]hould someone *other than a customer or authorized representative, like an imposter* or

[5] The insurer in *Universal*, National Union Fire Insurance Company of Pittsburgh, Pa., also urged the New York Court of Appeals to adopt *Morgan Stanley's* conclusion that both imposters and hackers are covered under the "fraudulent entry of data" language. Brief for Defendant-Respondent at 6-7, 21, *Universal*, 2015 WL 3885816.

hacker, input data into the Customer Communication System, it would constitute fraud and coverage is provided." *Id.* at *10 (emphasis added).[6]

That interpretation of the "fraudulent entry of data" language extends to "imposter" fraud is also consistent with Federal's understanding. Federal's underwriting corporate representative testified on behalf of the insurer that the Computer Fraud Coverage in the Policy is designed to cover "outside interlopers" seeking to cause a loss to Medidata. (Arehart Dep. 57:4-11, 59:2-10.) It was also acknowledged by Federal's claims representative, who conceded that the Computer Fraud Coverage would cover imposters to the extent the rest of the terms of the Computer Violation definition were met. (Maillet Dep. 170:7-17.)

Additionally, in *Universal*, the court noted as significant the fact that a computer system was not critical to the success of the fraud. 2015 WL 3885816 (coverage's "focus is on the computer system qua computer system"). Here, in contrast, it was the Computer System that provided the appearance of validity to the Imposter's email ([redacted] full name, email address and picture) as a result of it being manipulated by the Imposter's fraudulent entry of Data (the sender's email address). Absent Medidata's Computer System, there is no fraud here.

Federal's attempt to avoid coverage on the ground that the entry of the spoofed emails into Medidata's Computer System was "authorized" because the receiving inboxes were open to receive emails from any member of the public, (Ex. Stip. Ex. 12, at FIC000048), fares no better. In making that argument, Federal ignores the Policy language which is only concerned with whether there was a fraudulent "entry of" Data into a Computer System. Whether or not Medidata's Computer System was capable of receiving emails from anyone, the entry of the

[6] Federal is a subsidiary of the Chubb Group of Insurance Companies, *see* Chubb Subsidiaries, http://www.chubb.com/corporate/chubb11887.html (last visited Aug. 13, 2015), one of the defendant insurance companies who prevailed upon the court that the coverage applied to imposters. *See Morgan Stanley*, 2004 WL 5352285, at *7 ("[T]he Insurance Companies [including Chubb] denied Morgan Stanley's claim based on . . . the [policy] not being intended to cover a claim such as this, but directed toward 'imposters' or 'hackers,' . . . .").

fraudulent Data – "[redacted]" as the sender's address – into the Gmail system was unauthorized and fraudulent. To tell Medidata and other policyholders like it that Computer Fraud Coverage for which they paid substantial premiums is not available for fraud predicated on the vulnerabilities intrinsic to a Computer System like Google's Gmail, simply because their email inboxes can be accessed by the public without clear policy language to that effect would eviscerate the coverage Medidata purchased.

Finally, Federal's contention that the Policy language and the relevant case law "requires" a hacking incident for there to be coverage, (*id.* Ex. 15, at FIC000005), is without support in the Policy.[7] The Policy does not even use the word "hack" or "hacking." (Arehart Dep. 60:17-61:2; Maillet Dep. 167:2-10.) As the drafter of the Policy, Federal had ample opportunity to provide coverage solely for "hacking" had it intended to impose that limit on the coverage provided; having failed to do so, it cannot now be heard to ask the Court to read that narrowing language into the Policy by implication. *Cf. Vt. Teddy Bear Co. v. 538 Madison Realty Co.*, 1 N.Y.3d 470, 476 (2004) ("The parties could have negotiated and included an explicit notice requirement . . . . They did not do so."); *Bazin v. Walsam 240 Owner, LLC*, 72 A.D.3d 190, 195 (1st Dep't 2010); *Hartford Ins. Co. of the Midwest v. Halt*, 223 A.D.2d 204, 214 (4th Dep't 1996); *see also* 2 Couch on Insurance § 22.18 (3d ed. 2015). Instead, Federal used "fraudulent . . . entry of Data," which, as shown above, is exactly what took place in this case. And, contrary to Federal's reliance on *Universal* in this regard, the *Universal* trial court did not require "hacking" but instead merely used a hacker and imposter as examples to contrast with the fraudulent acts of authorized users not covered under the "fraudulent entry of data" language. *Universal*, 38 Misc. 3d at 863. *See also Owens, Schine & Nicola, P.C. v. Travelers*

[7] In addition, Federal never explains what it believes is "hacking" and why this manipulation of data to trick Medidata's Computer System into displaying false information does not constitute a hacking incident.

Cas. & Sur. Co. of Am., No. CV095024601, 2010 WL 4226958, at *7 (Conn. Super. Ct. Sept. 20, 2010) (finding that "Computer Fraud" coverage did not require a hacking incident to be triggered, with "Computer Fraud" defined as "[t]he use of any computer to fraudulently cause a transfer of Money . . ."), *vacated by stipulation of parties*, 2012 WL 12246940 (Conn. Super. Ct. Apr. 18, 2012).

The Imposter's emails effected the fraudulent entry of Data into Medidata's Computer System. Medidata's loss resulting therefrom should be covered as a matter of law.

B. Medidata's Loss Was Caused by Fraudulent Change to Data Elements in its Computer System

Medidata's claim for coverage also invokes, and is supported by, the second prong of the Computer Violation definition, which includes any "fraudulent . . . (b) change to **Data** elements." (Ex. Stip. Ex. 1, at FIC001343.) In a genuine email, the email address of the actual sender appears in the "From" line of the email. (Maillet Dep. 34:7-15.) Here, the perpetrators of the fraud caused the Gmail system to change information in the "From" line to reflect the email address of "[redacted]". (Maillet Dep. 78:4-15.) And, as a further result, the additional Data elements in the Gmail system – the display in the "From" line of the emails as they appeared to [redacted] and [redacted] of "[redacted]" and the inclusion of his picture – were fraudulently changed.

Federal has cited no case law in support of its denial of coverage under this prong of the Computer Violation definition. Rather it claims that although it does not know the specifics of how the fraud was perpetrated, (Maillet Dep. 158:24-159:4), its "understanding" is that the "From" line of the email was "populated" before the fraudulent emails were sent to Medidata.[8]

[8] If Federal is correct and the information was fraudulently manipulated before being sent to Medidata, the Data was therefore entered into the Computer System, satisfying the first prong of the Computer Violation definition.

(Ex. Stip. Ex. 15, at FIC000005.) Federal insists that it knows of no "facts that indicate that the name of the e-mail sender in the "From" box was changed." (*Id.*.)

That self-serving assertion ignores every undisputed fact known about the fraud, including the most basic facts that the Imposter, not [redacted], sent the emails, but that [redacted] name, email address and picture, not the Imposter's, nonetheless appeared in the "From" line. Even if the "From" line of the email was "populated" before the fraudulent emails were sent to Medidata, they were only "populated" with [redacted] email address; this had the effect of changing the Data elements in Medidata's Computer System – the addition of "[redacted]" and his picture to the displayed emails. (Watt Aff. ¶¶ 8, 10.)

The Imposter's emails effected the fraudulent change of Data elements in Medidata's Computer System. Medidata's loss resulting therefrom should be covered as a matter of law.

III. THE POLICY'S FUNDS TRANSFER FRAUD COVERAGE ALSO APPLIES TO MEDIDATA'S LOSS

As a matter of law and undisputed fact, the Fraud also falls within the Policy's Funds Transfer Fraud Coverage, as it (1) caused a direct loss of money; (2) by fraudulent electronic instructions purportedly issued by Medidata; (3) issued to a financial institution; (4) to deliver money from Medidata's accounts; (5) without Medidata's knowledge or consent. The Imposter utilized Medidata's employees as his conduit, and the electronic funds transfer was made without Medidata's knowledge or consent, falling squarely within this coverage grant.

Federal's only purported justification for it denial of coverage under this provision is its claim that because the payment instructions given JPMorgan Chase (the "financial institution"), were voluntarily given by Medidata employees (employees acting under the fraudulently-induced belief that the transactions had been authorized by [redacted]), those instructions were given with the "knowledge and consent" of Medidata. (*Id.* Ex. 12, at FIC000049; *id.* Ex. 15, at

FIC000005.) That position cannot withstand the slightest scrutiny, as [redacted] and [redacted] were manipulated by the Imposter, and were only "purportedly" acting on behalf of Medidata; they were the conduits for the fraudulent instructions. Indeed, there is no assertion that Medidata (the "Organization") believed there was a pending multimillion-dollar acquisition as to which it consented to the transfer of approximately $4.8 million consistent with the Imposter's instructions – the funds transfer was undisputedly without Medidata's knowledge or consent as required by the Policy. Having been duped and with their actions dictated by the Imposter, there can be no argument that [redacted] and [redacted] wire instructions were issued with Medidata's "knowledge and consent."

Federal's argument that the employees gave the transfer instruction to JPMorgan Chase voluntarily cannot make the fraud not covered, as that is what makes the transaction a "fraud" in the first place. If the employees had been under duress or were otherwise forced to give the transfer instruction, the Loss would not have resulted not from fraud, but from outright theft. The very nature of fraud is that it is accomplished by using a false premise to convince someone to voluntarily part with money or property. Thus, if the Funds Transfer Fraud Coverage provided under the Policy did not cover losses resulting from voluntary transfers Medidata was fraudulently induced to make, the coverage would be illusory.

And, the authority Federal cites supporting its funds transfer fraud coverage determination actually demonstrates why the language of Federal's Policy applies here. (Ex. Stip. Ex. 15, at FIC000005.) In *Cumberland Packing Corp. v. Chubb Insurance Corp.*, 29 Misc. 3d 1208(A), 2010 WL 3991185, at *5-6 (N.Y. Sup. Ct., N.Y. Cnty. Oct. 8, 2010), money the policyholder wired to Bernard Madoff was not covered by "Funds Transfer Fraud" coverage because Madoff was an authorized representative of the policyholder, and the policy contained

an authorized representative exclusion. There is no similar exclusion invoked here, and the Court should not imply an exclusion that does not exist.

Federal's reliance on *Pestmaster*, 2014 WL 3844627, at *5-6, is similarly unavailing as in that case the policy differed in a material respect that had the effect of eliminating coverage for Medidata's conduit-type fraud. The *Pestmaster* policy used the word "fraudulent" to modify the transmittal of the instruction – not the instruction itself. *Id.* at *4 ("[A]n . . . instruction *fraudulently transmitted* . . . which instruction purports to have been transmitted by you, but was in fact *fraudulently transmitted* by someone other than you . . . ." (emphasis added)). Medidata's Policy, in contrast, uses the word "fraudulent" to modify the "instructions." (Ex. Stip. Ex. 1, at FIC001345.) Had Federal wanted to limit the Funds Transfer Fraud Coverage to instances where the *transmittal* of the instructions was not authorized, it had to do so with language like that employed in *Pestmaster*. Here, all fraudulent instructions are covered no matter whether their transmittal was authorized or not. (*Id.*)

Here, the wire transfer instructions were undisputedly fraudulent. (*See* Maillet Dep. 42:15-43:11, 86:8-14 (acknowledging the emails constituted an instruction to do a wire transfer).) As a result, when the three Medidata employees, duped by the Imposter into acting as the Imposter's conduit, instructed JPMorgan Chase to send the $4,770,226.00 to the Imposter and his or her accomplices, Medidata suffered a covered Loss within the Policy's Funds Transfer Fraud Coverage. At the very least, the contrast with the language in *Pestmaster* and *Cumberland* renders the Policy ambiguous in this regard, which requires an interpretation in favor of Medidata. *See, e.g.*, *Morgan Stanley Grp.*, 225 F.3d at 275-76.

IV. THE POLICY'S FORGERY COVERAGE ALSO APPLIES TO MEDIDATA'S LOSS

Medidata is also entitled to summary judgment holding that its claim falls within the scope of the Policy's Forgery Coverage, which covers losses resulting from (1) the signing of the name of another natural person, with the intent to deceive; or (2) the alteration of a financial instrument. The perpetrators of the Fraud signed the name of another natural person when they affirmatively included the electronic signature[9] "[redacted]" or "[redacted]" at the end of each fraudulent email. (Ex. Stip. Ex. 3, at MED_0002113; *id.* Ex. 7, at MED_0002095; *id.* Ex. 9, at MED_0002089.) Because Medidata's Gmail system will only automatically add a signature to an email if it is sent using Medidata's email system on Google's servers (i.e. by the real [redacted]), (Watt Aff. ¶ 11), the perpetrators necessarily, affirmatively added his signature to each fraudulent email. This was done with the intent to deceive the Medidata employees into thinking they were corresponding with [redacted] and, ultimately, to deceive the employees into executing the transfer.

Federal has argued that there is no Forgery Coverage because the fraudulent emails do not meet the Policy definition of a Financial Instrument. (Ex. Stip. Ex. 12, at FIC000048; *id.* Ex. 15, at FIC000006.) While that is incorrect – the definition of Financial Instrument includes an "order or direction to pay a sum certain in Money" (*id.* Ex. 1, at FIC001345) – it is also irrelevant, because the Policy requires only that there be either a Forgery (as defined therein) *or* an alteration of a Financial Instrument. (*Id.* at FIC001342.)[10] Because there was a Forgery as

[9] The Policy specifically provides that "[m]echanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures." (Ex. Stip. Ex. 1, at FIC001345.)

[10] Again, to the extent this provision is found to be ambiguous, since it, like the entire Policy, was drafted by Federal, it must be construed in favor of Medidata and coverage. *See, e.g.*, *Morgan Stanley Grp.*, 225 F.3d at 275-76.

defined by the Policy, there does not need to be alteration of a Financial Instrument, and this grant of coverage provides a third basis to cover Medidata's loss under the Policy.[11]

CONCLUSION

For the reasons stated above, Medidata's motion for summary judgment should be granted.

Dated: New York, New York
August 13, 2015

KASOWITZ, BENSON, TORRES & FRIEDMAN LLP

By: _____

Robin L. Cohen (rcohen@kasowitz.com)
Adam S. Ziffer (aziffer@kasowitz.com)
Alexander M. Sugzda
(asugzda@kasowitz.com)

1633 Broadway
New York, New York 10019
Tel: (212) 506-1700
Fax: (212) 506-1800

Attorneys for Plaintiff Medidata Solutions, Inc.

[11] The Policy's "Limits of Liability and Retention" section provides "If a loss is covered under more than one Insuring Clause, the maximum amount payable under this coverage section shall not exceed the largest applicable Limit of Liability of any such Insuring Clause." (Ex. Stip. Ex 1, at FIC001354.) The Policy thereby explicitly recognizes the possibility of overlapping coverage.